AIR WAR COLLEGE

AIR UNIVERSITY

THE BEST DEFENSE IS A GOOD OFFENSE:

CONDUCTING OFFENSIVE CYBEROPERATIONS AND THE LAW OF ARMED CONFLICT

by

Vito Smyth, Lieutenant Colonel, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Kimberly A. Hudson, PhD.

13 February 2014

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Vito Smyth is assigned to the Air War College, Air University, Maxwell AFB, Alabama. Prior to his current assignment, Lieutenant Colonel Smyth was commander, 22d Medical Support Squadron, McConnell AFB, Kansas. He has also served as an Air Force Legislative Fellow in the office of United States Senator Daniel Akaka (Hawaii); branch chief in the office of the Secretary of the Air Force, Legislative Liaison; and as a senior research analyst for the congressionally directed Task Force on the Future of Military Health Care. After earning a Bachelor of Science in Business and Management from the University of Maryland and a Juris Doctor from Cleveland State University, he received a direct commission in the United States Air Force Medical Service Corps. Lieutenant Colonel Smyth has served in a variety of other healthcare administration command, leadership, and legislative liaison positions at the installation, Air Staff and Joint levels. He also earned a Master of Health Administration from Baylor University in 2004. Lieutenant Colonel Smyth is admitted to the practice of law in Ohio and to the bars of the Supreme Court of the United States, the United States Court of Appeals for the Sixth Circuit, and the United States Court of Appeals for the Armed Forces. He is also a Fellow of the American College of Healthcare Executives.

Abstract

The National Defense Authorization Act for Fiscal Year 2012 gave the Department of Defense the statutory authority to conduct offensive cyberoperations, subject to the Law of Armed Conflict. Four major types of offensive cyberoperations include destroying data on a network or a system connected to a network, being an active member of a network and generating bogus traffic, clandestinely altering data in a database stored on a network and degrading or denying service on a network. Conducting these operations, as opposed to cyberexploitation, will require military planners to analyze potential actions through the lens of the Law of Armed Conflict's constraint elements of military necessity, proportionality, perfidy, distinction and neutrality. The use of a recognized analytical framework lends legitimacy to actions undertaken by the United States, and shows a continued commitment to recognized rules of international law. Utilizing the present parameters of the existing LOAC framework, parallel legal and historical analogies and reasonable interpretations and applications of those analogies, the United States should legitimately be able to conduct the four types of offensive cyberoperations.

Introduction

On August 7, 2008, the country of Georgia launched an invasion into South Ossetia in response to growing tension with Russia over the disputed region's future.[1] This conflict had its roots in, inter alia, Georgia's loss of South Ossetia to Russia in 1992 and the subsequent installation of unrecognized pro-Russian governments.[2] The war proceeded down a recognized path of small wars between nation states. Georgian forces began an artillery attack against a major town in the South Ossetia region, and the Russians responded with a naval blockade of Georgian ports, the deployment of combat troops in South Ossetia and bombing missions into Georgia.[3] Russia soon gained the upper hand, and after five days of fighting an EU brokered ceasefire took effect.[4] Besides Georgia's failure to capture South Ossetia, the war resulted in over 100,000 displaced civilians, 400 civilians killed and 200 Georgian and 64 Russian military casualties.[5] Both sides continued to blame each other for provoking the war.[6]

At first blush, this war seems rather unremarkable. However, this was a war unlike any other. According to David Hollis, "this appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains (consisting of land, air, sea, and space)."[7] From pre-invasion streams of data containing

[1] David Hollis, *Cyberwar Case Study: Georgia 2008*, Small Wars Journal Blog (January 6, 2011) found at http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008, 1.

[2] Ibid.

[3] Ibid.

[4] Paul Ames, "EU: Most Russian cease-fire allegations overblown," *USA Today*, 24 October 2008, http://usatoday30.usatoday.com/news/world/2008-10-24-2937695828_x.htm (accessed 29 October 2013).

[5] Bruno Waterfield, "EU blames Georgia for starting war with Russia," *The Telegraph*, 30 September 2009, http://www.telegraph.co.uk/news/worldnews/europe/georgia/6247620/EU-blames-Georgia-for-starting-war-with-Russia.html (accessed 29 October 2013).

[6] C.J. Chivers, "Georgia Offers Fresh Evidence on War's Start," *New York Times*, 15 September 2008, http://www.nytimes.com/2008/09/16/world/europe/16georgia.html?_r=2&oref=slogin& (accessed 29 October 2013).

[7] Hollis, 2.

"win+love+in+Rusia" directed towards Georgian government sites[8] to coordinated attacks overloading and disabling Georgian servers,[9] the U.S. Cyberconsequences Unit report noted Russian organized crime and other civilians, without any apparent direct links to the Russian military or government, carried out much of the cyberattacks against the Georgian government.[10] The same report noted "54 web sites in Georgia related to communications, finance, and the government were attacked by rogue elements within Russia. The bad guys weren't working for the Russian government or military but it is safe to say that there had to be some complicity here."[11] Also, "experts say evidence suggests that Russian officials did little to discourage the online assault, which was coordinated through a Russian online forum that appeared to have been prepped with target lists and details about Georgian Web site vulnerabilities well before the two countries engaged in a brief but deadly ground, sea and air war."[12]

This war will not be the last of its type. Why? Cyberattacks enjoy two significant advantages. Namely, they are relatively cheap to employ, and it is nearly impossible to determine responsibility for them.[13] Bill Woodcock, the research director at Packet Clearing House, a nonprofit internet research organization, remarked "you could fund an entire cyberwarfare campaign for the cost of replacing a tank tread, so you would be foolish not to."[14]

[8] John Markoff, "Before the Bombs, Cyberattacks." *New York Times*, August 13, 2008, sec. A1.
[9] Ibid.
[10] Mark Rutherford, "Report: Russian mob aided cyberattacks on Georgia," *CNET News* (18 August 2009) found at http://news.cnet.com/8301-13639_3-10312708-42.html (accessed on 29 October 2013).
[11] Jon Oltsik "Russian Cyber Attack on Georgia: Lessons Learned?" *Network World*, (17 August 2009), found at: http://www.networkworld.com/community/node/44448 (accessed on 29 October 2013).
[12] Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post* (16 October 2008), found at http://voices.washingtonpost .com/securityfix/2008/10/report_russian_hacker_forums_ forums_f.html (accessed on 29 October 2013).
[13] Markoff, "Before the Bombs, Cyberattacks," A1.
[14] Ibid.

The United States has embraced the idea of conducting offensive cyberwarfare.[15] Offensive cyberoperations, "executed by DoD's Cyber Command, either in support of conventional, kinetic war fighting or on a stand-alone basis"[16] is one relatively new tool in the military instrument of power toolbox. Steven Bradbury underscores "the fact that the (Obama) administration is standing up a unified Cyber Command and putting such focus and resources into it suggests that the President has largely decided to conduct offensive cyber operations through the military option."[17] So, given the fact that there is statutory authority to conduct offensive cyberoperations as well as a significant investment in doing so, should one look at the legal underpinnings of fighting a war in this brave, new domain? The very statutory authority that allows the Department of Defense to conduct offensive operations in cyberspace also places on it the burden to observe "the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict."[18] This research paper will look at conducting offensive cyberoperations thru the lens of the Law of Armed Conflict (LOAC). First, I'll discuss LOAC. Second, I'll explain offensive cyberoperations, and differentiate between cyberattack and cyberexploitation, Next, I'll identify four types of offensive cyberoperations. Finally, I'll use the LOAC elements of constraint to analyze the utility and propriety of offensive cyberoperations.

[15] National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, §954, 125 Stat. 1298, 1551 (2011). "Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to—(1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution (50 U.S.C. §1541 et seq.)."

[16] Steven G. Bradbury, "Keynote Address: The Developing Legal Framework for Defensive and Offensive Cyber Operations," *Harvard National Security Journal*, vol. 2: 591, 602 (2011).

[17] Ibid., at 607.

[18] National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, §954, 125 Stat. 1298, 1551 (2011). See Note 15.

Thesis

This research paper uses a qualitative approach to argue that the United States should be able to conduct offensive cyberoperations within the *jus in bello* parameters of the Law of Armed Conflict.

Foundational Assumptions

It is important at the outset to establish some assumptions of this paper. First, the main body of relevant international laws, and the body of laws most pertinent for the discussion of this paper, is LOAC.[19] Second, offensive cyberoperations during a state of international armed conflict between two state actors will be examined. Therefore only the portions of the LOAC (*jus in bello*) that address ongoing hostilities will be explored.[20] Third, the effects rather than the modality of offensive cyberoperations are the appropriate starting point for understanding how LOAC applies to it.

[19] For further discussion on ethical frameworks such as the Just War Theory applicability to cyberwarfare, see Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* vol. 9, #4: 384 (2010), and Cook's reply at James Cook, "Cyberation and Just War Doctrine: A Response to Randall Dipert," *Journal of Military Ethics* vol. 9, #4: 411 (2010) as well as Kristen Tullos, *Symposium: International Law and The Internet: Adapting Legal Frameworks in Response to Online Warfare and Revolutions Fueled by Social Media: From Cyber Attacks to Social Media Revolutions: Adapting Legal Frameworks to the Challenges and Opportunities of New Technology*, Emory International Law Review vol. 26: 733 (2012), citing Eric Talbot Jensen, *Cyber Deterrence*, Emory International Law Review vol. 26: 773 (2012).

[20] For non-state actor involvement in offensive cyberoperations, see Erick Mudrinich, *Article: Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, Air Force Law Review vol. 68: 167 (2012).

The Law of Armed Conflict (LOAC)

LOAC addresses two fundamental questions regarding the conduct of armed conflict. First, when can a nation state legally use force against another; and second, once hostilities have commenced, what are the set of rules that govern the nation state belligerents?[21] *Jus ad bellum* is the set of laws that apply when one nation state can legally use force against another.[22] Put another way, it refers to "those established 'conflict management' norms and procedures that dictate when a state may--and may not--legitimately use force as an instrument of dispute resolution."[23] The law governing when nations are involved in international armed conflict, which is wholly distinct and separate from *jus ad bellum*, is known as *jus in bello*.[24] The Hague Conventions of 1899 and 1907, the Geneva Conventions and customary international law serve as foundational support of modern *jus in bello* interpretations.[25] Customary international law is one of two sources of international law, with the other source being treaties.[26] Customary international law springs "from a general and consistent practice of states followed by them from a sense of legal obligation."[27] Bradley and Goldsmith note that "despite its relatively amorphous nature, CIL [customary international law] has essentially the same binding force under international law as treaty law."[28]

[21] Anna Wortham, *Note: Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?* Federal Communications Law Journal vol. 64: 643, 646 (May 2012).

[22] Ibid.

[23] Ibid.

[24] George K. Walker, *Information Warfare and Neutrality*, Vanderbilt Journal of Transnational Law vol. 33 no. 5: 1079, 1090 (November 2000).

[25] William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, DC: National Academics Press, 2009), 246.

[26] Curtis A. Bradley and Jack L. Goldsmith, *Customary International Law as Federal Common Law: A Critique of the Modern Position*, Harvard Law Review vol. 110, no. 4: 815, 817 (February 1997).

[27] Louis Henkin, ed. *Restatement of the Law Third, The Foreign Relations Law of the United States* (Philadelphia, PA: American Law Institute, 1989), §102(2).

[28] Bradley and Goldsmith, 818, citing *Restatement of the Law Third, The Foreign Relations Law of the United States*, §102, comment j.

Offensive Cyberoperations, Cyberattack and Cyberexploitation

Offensive cyberoperations cover a wide range of computer-based activities aimed at disabling or disrupting an adversary's ability to use computer based resources or assets or to defend a nation's own network against exploitation. Offensive cyberoperations can range from activities such as collecting or copying data from foreign computer systems and databases to disrupting computer systems, denying its use by others and even covert action conducted by intelligence agencies aimed at damaging an adversary's computer systems.[29] As noted earlier, offensive cyber operations will primarily be conducted through the military instrument of power.[30] Given this current military emphasis buttressed by the fact that the military now has the statutory authority to conduct offensive cyberoperations, it will be vitally important for planners and executors of these operations to know the operational parameters to ensure the legitimacy of their actions and resultant consequences.

The terms cyberattack and cyberexploitation are often used interchangeably, but they are different. Wortham points out that "cyber attacks and cyber exploitations are the two forms of hostile actions that may be taken against a computer system or network. Cyber-attack and cyber exploitation are two distinct actions."[31] Cyberattack refers to refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[32] One of the objects of cyberattacks is to make an adversary think that their computer systems or data related to those systems are unreliable or unavailable for use, thereby degrading an adversary's ability to conduct

[29] Steven G. Bradbury, *Keynote Address: The Developing Legal Framework for Defensive and Offensive Cyber Operations*, Harvard National Security Law Journal vol. 2: 591, 602 (2011).

[30] Ibid., at 607.

[31] Anna Wortham, *Note: Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?* Federal Communications Law Journal vol. 64: 643, 646 (May 2012).

[32] Owens, Dam and Lin, 10-11.

armed conflict effectively.[33] Cyberexploitation is usually conducted for the "purpose of obtaining information resident on or transiting through an adversary's computer systems or networks."[34] Wortham notes that "the main difference between cyber-attack and cyber exploitation is that cyber-attack is destructive in nature while cyber exploitation is focused on intelligence gathering and, in order to be covert, purposely does not try to affect the normal processes of the computer or network exploited."[35] In fact, "the best cyberexploitation is one that such a user never notices."[36]

[33] Wortham, 646.
[34] Owens, Dam and Lin, 11.
[35] Wortham, 646.
[36] Owens, Dam and Lin, 11.

Four Types of Offensive Cyber Operations

For purposes of this paper, I will confine offensive cyberoperations to four general types of actions. They are destroying data on a network or a system connected to a network, being an active member of a network and generating bogus traffic, clandestinely altering data in a database stored on a network and degrading or denying service on a network. I'll briefly describe each one of these types of actions.

Destroying Data on a Network or a System Connected to a Network

The first type of offensive cyberoperation is destroying data on a network or a system connected to a network. In this type of offensive cyberoperation, a belligerent gains access to an enemy's network to delete data or reformat files found on system hard drives.[37] This type of offensive cyberoperation could cripple any sort of function whose proper operation depends on being connected to a network or data connected to a network, such as a power grid.[38]

Being an Active Member of a Network and Generating Bogus Traffic

The second type of offensive cyberoperation is being an active member of a network and generating bogus traffic. In this type of offensive cyberoperation, a belligerent gains access to an adversary's network and masquerades as a trusted person or source.[39] An example might be a belligerent who may "masquerade as the adversary's national command authority or as another senior official or agency and issue phony orders or pass faked intelligence information."[40]

Clandestinely Altering Data in a Database Stored on a Network

The third type of offensive cyberoperation is to clandestinely alter data in a database stored on a network. In this type of offensive cyberoperation, a belligerent gains access to an

[37] Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, Journal of National Security Policy Law, vol. 4: 63, 69-70 (2010).
[38] Ibid.
[39] Ibid.
[40] Ibid.

adversary's network and changes, but doesn't destroy, data stored on a database or a network.[41] An example might be a belligerent gaining access to a database of aircraft parts and changing the condition codes on various items to wrongly reflect that unserviceable items are serviceable and could be used to repair jet engines.

Degrading or Denying Service on a Network

The fourth type of offensive cyberoperation is to degrade or deny service on a network. In this type of offensive cyberoperation, a belligerent attempts "to degrade the quality of service available to network users by flooding communications channels with large amounts of bogus traffic."[42] An example is an e-mail server being flooded with so many e-mail messages that the server crashes and becomes inoperable.

[41] Ibid.
[42] Ibid.

LOAC Elements of Constraint Analysis of Offensive Cyberattacks

Owens, Dam and Lin lay out six modern constraints categories and definitions on the conduct of belligerents during international armed conflict. These constraints are military necessity, proportionality, perfidy, distinction, neutrality and discrimination. They serve as a useful analytical framework to determine the propriety of conduct when nation states are engaged in various operations of armed conflict, including offensive cyberoperations. I will utilize this framework, albeit with one minor modification.

Military Necessity

Military necessity demands that valid targets are limited to those that make a direct contribution to the enemy's war effort, or those whose damage or destruction would produce a military advantage because of their nature, location, purpose, or use, or in other words, a military objective.[43] Schmitt asserts the problem regarding interpreting what is a "military objective" "lies in ascertaining the required nexus between the object to be attacked and military operation."[44] The International Committee of the Red Cross (ICRC) narrowly defines the definition of military necessity contained in Geneva Convention Additional Protocol.[45] [46] According to Schmitt, the ICRC's Commentary to the Protocol would exclude "attacks that offer only a 'potential or indeterminate' advantage" as not establishing a clear military-civilian nexus justifying military necessity.[47][48] Schmitt notes that the United States takes a different tack on the

[43] Owens, Dam and Lin, 246.

[44] Michael N. Schmitt. *Wired Warfare: Computer Network Attack and Jus in Bello*. International Review of the Red Cross vol.84, no. 846: 365, 380 (2002).

[45] Ibid.

[46] Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Art. 52(2), 12 December 1977. (downloaded 10 November 2013 at http://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=F08A9BC78AE360B3C12563CD0051DCD4). "Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture."

[47] Schmitt, 380.

interpretation of military objective. The U.S would include economic targets that "indirectly but effectively support and sustain the enemy's war-fighting capability, a particularly expansive interpretation."[49] This expansive interpretation is also reflected in joint doctrine as reflected in Joint Publication 3-60, which engenders "debates about attacks on enemy morale, information operations, interconnected systems, and strategic versus tactical-level advantages, to name a few areas."[50]

For all four types of offensive cyberoperations, the analysis is the same: does the targeted system bear some nexus between the object to be attacked and military operation given the United States expansive definition of military objective? As more and more of a country's economy become dependent on the internet, from purely a military objective standpoint this may broaden the amount of targets that can be pursued by American offensive cyberoperations. Indirect targets such as financial institutions that support an enemy's military operations, energy sources used to sustain military operations and other institutions that provide support to an armed conflict could be targeted. There may be other legal and political considerations that would militate attacking such targets, but from a military objective standpoint these would be legitimate targets for offensive cyberoperations. However, there are limits to what may be considered as acceptable targets. For example, attacking networks associated with certain categories of objects, such as religious and medical buildings and infrastructures would be prohibited since they enjoy

[48] Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ICRC, Geneva, 1987, para. 2024, (downloaded 10 November 2013 at http://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?viewComments=LookUpCOMART&articleUNID=F08A9BC78AE360B3C12563CD0051DCD4). "Finally, destruction, capture or neutralization must offer a ' definite military advantage ' in the circumstances ruling at the time. In other words, it is not legitimate to launch an attack which only offers potential or indeterminate advantages. Those ordering or executing the attack must have sufficient information available to take this requirement into account; in case of doubt, the safety of the civilian population, which is the aim of the Protocol, must be taken into consideration."

[49] Schmitt, 380-381, citing The Commander's Handbook on the Law of Naval Operations (NWP 1-14M, MWCP 5-2.1, COMDTPUB P5800.7), para 8.1.1 (1995).

[50] Law of Armed Conflict Deskbook, International and Operational Law Department, (Charlottesville, VA: The United States Army Judge Advocate General's Legal Center and School, 2012), 138.

special protection and under usual circumstances are immune from being targeted by belligerents.[51]

Proportionality

Proportionality determinations are analyzed through the prism of the Geneva Convention Additional Protocol. "An attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" violates the principle of proportionality. [52] Proportionality would not, per se, prohibit the use of the four types of offensive cyberoperations. Rather, "the prohibition is on the death, injury, and destruction being excessive; not on the attack causing such results."[53]

Proportionality should also be examined from the doctrine of Double Effect standpoint. Walzer explains than when military planners consider attacking a target, the attacker must intend to hit the target, and that the attacker must not intend to harm civilians.[54] In fact, Walzer stresses that "it is morally necessary to take such measures, that is, to be careful in the strongest sense, even if it appears likely that the number of deaths caused by the attack would not be

[51] (Look at footnote 47 format) The 1949 Geneva Convention I, Article 19: "Fixed establishments and mobile medical units of the Medical Service may in no circumstances be attacked, but shall at all times be respected and protected by the Parties to the conflict. Should they fall into the hands of the adverse Party, their personnel shall be free to pursue their duties, as long as the capturing Power has not itself ensured the necessary care of the wounded and sick found in such establishments and units. The responsible authorities shall ensure that the said medical establishments and units are, as far as possible, situated in such a manner that attacks against military objectives cannot imperil their safety."

[52] Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Art. 51(5), 12 December 1977. (Downloaded 16 November 2013 at http://www.icrc.org/ihl/WebART/470-750065).

[53] Law of Armed Conflict Deskbook, International and Operational Law Department, The United States Army Judge Advocate General's Legal Center and School, Charlottesville, VA (2012), 149.

[54] Michael Walzer, "Responsibility and Proportionality in State and Nonstate Wars," *Parameters* vol. 39: 48-49 (Spring 2009).

'disproportionate to' whatever the relevant measure might be. The attacking force must protect civilians as best they can—period. That is their moral responsibility."[55]

Schmitt notes two problems concerning offensive cyberoperations and proportionality. "A balance must be struck between suffering and damage versus military advantage without a common system of valuation. There aren't any 'right' answers, and the answers are always contextual depending on what is going on at the time of hostilities." [56] The Commentary to the Additional Protocols note the difficulty and ambiguity as well, saying "putting these provisions into practice, or, for that matter, any others in Part IV, will require complete good faith on the part of the belligerents, as well as the desire to conform with the general principle of respect for the civilian population."[57]

The proportionality analysis is also made more difficult by the possibility of second-tier effects. "The secondary effects of a cyber attack can be profound and, depending on whether the attack extends beyond its intended target in a significant way, can violate the principle of proportionality; therefore, one should not trivialize its impact in a time of war."[58] However, Richardson points out that in the cyber realm, direct injury, death, damage, or destruction from an attack is rare - at least as of 2011 - whether aimed at civilian or military objectives. Direct harm to people from a virus infecting a computer - as distinguished from a denial of service attack - has not been documented."[59] In addition, Schmitt points out that the use of offensive cyberoperations may actually work to decreasing the size and scope of collateral damage and

[55] Ibid., 49.
[56] Schmitt, 392.
[57] Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ICRC, Geneva, 1987, para. 1978 (Downloaded 16 November 2013 at http://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?viewComments=LookUpCOMART&articleUNID=4BEBD9920AE0AEAEC12563CD0051DC9E).
[58] John Richardson, *Article: Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, John Marshall Journal of Computer & Information Law vol. 29: 1, 24 (Fall, 2011).
[59] Ibid.

incidental injury by merely "turning off" or interrupting an enemy's target as opposed to destroying it.[60] Instead of bombing an airfield, air traffic control can be interrupted for short periods of time. The same is true for power production, distribution and communication systems and industrial plants. Interrupted or turned off functions can be brought back online soon after the need for its inability to operate is over, thereby minimizing the deleterious effects on the civilian population and obviating the need to rebuild destroyed facilities.[61]

Perfidy

When a belligerent "seeks to deceive an enemy into believing that he is obligated under the law of armed conflict to extend special protection to a friendly asset when such is not the case," the belligerent commits the prohibited act of perfidy.[62] Such a violation is considered a "grave breach" of international law.[63] Certain categories of objects and people, such as religious buildings, medical facilities medical personnel and prisoners of war, enjoy special protection and must be identified as such to prevent other belligerents from identifying and targeting them as legitimate military targets.[64] When a belligerent intentionally misuses these markings and symbols for protected persons or objects, that belligerent is guilty of perfidy.[65] It is important to distinguish perfidy from lawful ruses. A lawful ruse is "intended to mislead an adversary or to induce him to act recklessly but is use infringes no rule of international law applicable in armed conflict and doesn't mislead the adversary into believing that he is entitled to special

[60] Schmitt, 394.
[61] Ibid.
[62] Ibid.
[63] Louis René Beres, *Religious Extremism and International Legal Norms: Perfidy, Preemption, and Irrationality*, Case Western Reserve Journal of International Law, vol. 39: 709, 722 (2007-2008).
[64] Owens, Dam and Lin, 247.
[65] Ibid.

protection."[66] Common, lawful ruses include decoys, fake operations, camouflage and misinformation.[67]

Conducting offensive cyberoperations offers many opportunities for ruses and perfidy. Being an active member on a network and transmitting bogus traffic as well as clandestinely altering data in a database or a database connected to a network can be used to transmit or convey false information. "Lawful ruses might include transmitting false data meant to be intercepted by an adversary that relate to troop deployments or movements. Another example could be altering an adversary's database, resulting in sending messages to enemy headquarters purporting to be from subordinate units, or passing instructions to subordinate units that appear from their headquarters."[68] However, depending on how offensive cyberoperations are implemented, perfidy can occur. "Medical units and transports may use codes and signals established by the International Telecommunications Union, the International Civil Aviation Organization, and the International Maritime Consultative Organization to identify themselves. Falsely transmitting such codes or signals, or causing an adversary system to reflect such false signals (through being an active member of a network and generating bogus traffic or clandestinely altering data in a database or a database connected to a network) would be examples of perfidy."[69] Military planners should take caution in being an active member of a network and generating bogus traffic or clandestinely altering data in a database or a database connected to a network so that they can take advantage of legal ruses, and not cross the line into perfidy. For example, using visual morphing techniques to create an image of the enemy's chief

[66] Ibid.
[67] Ibid.
[68] Ibid., 395.
[69] Ibid.

of state informing his forces that an armistice or cease-fire agreement had been signed would be a war crime according to the Department of Defense.[70]

Distinction

The principle of distinction requires belligerents to "make reasonable efforts to distinguish between military and civilian assets and between military personnel and civilians, and to refrain from deliberately attacking civilians or civilian assets."[71] The 1977 Additional Protocol I to the Geneva Convention[72] illustrates the principle of distinction: "[A] technical term in the laws of armed conflict intended to protect civilian persons and objects. Under this principle, parties to an armed conflict must always distinguish between civilians and civilian objects on the one hand, and combatants and military targets on the other."[73] Kelsey's analysis of distinction with regard to the use of offensive cyberoperations would be similar to the use of kinetic weapons, and would be permissible in most situations.[74] "As militaries develop plans for using cyber weapons, the military and legal communities will need to reinterpret the principle to effectively apply it to cyber warfare. This process seems relatively straightforward for most uses of cyber weapons."[75]

Dual use objects, or those that serve both military and civilian objectives such as rail lines, power grids, communications systems, and factories, "qualify as military objectives subject

[70] Ibid., 395-396.
[71] Ibid.
[72] Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Art. 57, 12 December 1977. (Downloaded 16 November 2013 at http://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?key=distinction&action=openDocument&documentId=50FB5579FB098FAAC12563CD0051DD7C).
[73] Heike Spieker, "Civilian Immunity." *Crimes of War: What the Public Should Know*. Roy Gutman and David Rieff, eds. (New York: W.W. Norton and Company, 1999), p. 84.
[74] Jeffrey T.G. Kelsey, Note, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyberwarfare, Michigan Law Review, vol. 106: 1427, 1437 (2008).
[75] Ibid.

to attack, even if their primary purpose is not military, but civilian."[76] Schmitt, like Hollis, takes a broad interpretation of dual use objects, stating "if an object is being used for military purposes, it is a military objective vulnerable to attack, including computer network attack. This is true even if the military purposes are secondary to the civilian ones."[77] This expansive interpretation would give military planners the flexibility to employ offensive cyberoperations against the full array of dual use objects. However, some caveats should be noted. Because distinction requires that "make reasonable efforts to distinguish between military and civilian assets and between military personnel and civilians,"[78] offensive cyberoperations that could cause civilian death and destruction would not be permitted because at a minimum, international humanitarian law requires military commanders to "know not just where to strike but be able to anticipate all the repercussions of an attack."[79] For example, if conducting any type of offensive cyberoperation would have the effect of disrupting an air traffic control system that could endanger relief planes or commercial aircraft, "the principle of distinction would force the commander to evaluate whether such a plan was the best way to achieve the expected military advantage while minimizing the loss of civilian lives. Again, the principle would likely dictate a change to the scope of the operation to avoid the threat to civilians."[80] Therefore, offensive cyberoperations that target dual use objects need to be analyzed in the same way that dual use targets are analyzed when kinetic weapons are used.[81]

[76] Hollis, at 1044.
[77] Schmitt, 384.
[78] Owens, Dam and Lin, 247.
[79] Bradley Graham, "Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia," *Washington Post*, Nov. 8, 1999, A1.
[80] Kelsey, at 1438.
[81] "Where infrastructures have a "dual-use" serving both civilian and military purposes—they qualify as military objectives subject to attack, even if their primary purpose is not military, but civilian. If that rule holds for IO, however, then militaries may target virtually all computer networks. As of 2000, 95% of all U.S. military traffic moved over civilian telecommunication and computer systems, and the trend is clearly towards greater consolidation of civilian and military technology. The dual-use rule suggests, therefore, that U.S. adversaries may treat all U.S.

Some commentators (such as Owens, Dam and Lin, *supra*) differentiate between the terms distinction and discrimination. However, both terms are essentially synonymous. Discrimination places the obligation upon belligerents to use weapons and tactics only against combatants and to avoid non-combatants.[82] Certain weapons, such as biological and chemical weapons, have been banned by treaty due to their indiscriminate nature.[83] It's important to note that there isn't a blanket ban on all indiscriminate weapons since "the harm to non-combatants is minimized through adherence to the requirements of proportionality."[84]

Presently, there are no agreements among nations banning the conduct of offensive cyberoperations. Russia has advocated for an international agreement that would ban the use of cyberweapons since military activities are increasingly being conducted on civilian information networks.[85] The United States has resisted for such a call, "arguing that it was impossible to draw a line between the commercial and military uses of software and hardware."[86] Leaven and Dodge argue that the United States' response to cyberattack would be handcuffed by the restrictions of an international treaty as well as threaten its leadership in cyberspace.[87] In short, the prospects for an international treaty addressing the use of offensive cyberoperations appear dim.

---

communication systems as military objectives and attack them by IO or kinetic means. Thus, application of the civilian distinction principle to IO not only involves uncertainty, it also suggests increasing tension with the principle's purported goal of restricting military attention on civilians and their property as much as possible during conflict." Hollis, at 1044 (Internal citations omitted).

[82] Richard DiMeglio, *The Evolution of the Just War Tradition: Defining Jus Post Bellum*, Military Law Review vol. 186: 116, 130 (2005).

[83] Owens, Dam and Lin, 249-250.

[84] Ibid., 250.

[85] Gabriel K. Park, *Note: Granting an Automatic Authorization for Military Response: Protecting National Critical Infrastructure from Cyberattack*, Brooklyn Journal of International Law, vol. 38: 797, 815-816 (2013).

[86] John Markoff and Andrew E. Kramer, "In Shift, U.S. Talks to Russia on Internet Security," *New York Times*, December 12, 2009, A1. (Downloaded November 29, 2013 at http://www.nytimes.com/2009/12/13/science/13cyber.html?scp=l&sq=u.s.%20%20talks%20to%20russia%20on%20web%20security&st=cse.&_r=0).

[87] Tod Leaven and Christopher Dodge, *The United States Cyber Command: International Restrictions vs. Manifest Destiny*, North Carolina Journal of Law & Technology, vol. 12: 1 (2010).

Neutrality

A nation can, under customary international law, "refrain from taking part in an armed conflict or war by declaring neutrality or otherwise assuming neutral status."[88] Once a nation declares its neutrality or assumes a neutral status, it is legally protected from being attacked or having its territorial integrity violated by belligerents as long as it does not take part in the armed conflict between the belligerents.[89] Walker notes that "LOAC treats neutrals' rights and duties differently, depending on the modality of warfare and the part of the Earth affected, such as neutral lands, neutral oceanic waters, the high seas or neutral airspace. There is overlap between the different systems,"[90] an important point to note especially in offensive cyberoperations.

Offensive cyberattacks that are carried out via the internet are likely to "involve message traffic that physically transits a number of different nations. Moreover, it is entirely possible, likely even, that [nations not involved in hostilities] would be aware of the fact that they were carrying attack traffic at all."[91] If the United States decides to conduct offensive cyberoperations via the internet, these operations will most likely be conducted thru servers and information pipelines that transit neutral nations, or at the very least through nations not involved in the armed conflict as belligerents. Given the unique and ubiquitous nature of offensive cyberoperations, what obligations would a belligerent have in not routing an offensive cyberoperation through a neutral nation's routers, servers and information infrastructure? To answer that question, one has to look at the existing governing law.

[88] George K. Walker, *Information Warfare and Neutrality*, Vanderbilt Journal of Transnational Law, vol. 33, no. 5: 1079, 1143 (November 2000).
[89] Owens, Dam and Lin, 247-248.
[90] Walker, 1146.
[91] Owens, Dam and Lin, 268.

Walker posits that the laws of naval and air warfare are perhaps the best sources of correlative law when applied to the conduct of offensive cyberoperations.[92] He notes that since the geographic environment of the sea and air and the virtual environment of the Internet are fluid and that no nation can claim sovereignty over vast stretches of the sea and air as well as the Internet, naval and air warfare law probably are the best sources from which to draw parallels.[93] A good example is the "Hague Radio Rules," a set of naval warfare laws that deal with the information transmission "concerning military forces or operations destined for a belligerent."[94] Drawing an analogy, Walker advocates "the correlative right of a belligerent that is aggrieved by [information warfare] incursions should be that the belligerent may take such actions as are necessary in the context of a neutral that is unable (or perhaps unwilling) to counter enemy [information warfare] force activities making unlawful use of that territory."[95] As a result, a nation conducting offensive cyberoperations may put neutral nations at risk of attack.

Drawing parallels from others sources of law can also produce a dissimilar conclusion. Owens, Dam and Lin point out that under the Hague Convention of 1907 provisions addressing telephone and telegraph communications, "a neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[96] By implication, if a neutral nation doesn't have a duty to interfere with the transit of information on telephone or telegraph cables, then "an analyst might conclude that belligerents do not have the right to interfere with

[92] Walker, 1199.
[93] Ibid.
[94] Ibid., 1158.
[95] Ibid., 1199.
[96] Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land. The Hague, 18 October 1907, (downloaded November 29, 2013 at http://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=3F3777763877124FC12563CD005169EB).

nodes located in the neutral nation."[97] While contrary conclusions can be drawn, there is still a valid justification to launch offensive cyberoperations without violating a neutral nation's non-belligerent status.

[97] Owens, Dam and Lin, 270.

Recommendations

Given the presence of an internationally recognized framework in which to conduct military operations, the United States should continue to utilize the LOAC as a basis from which to conduct the four types of offensive cyberoperations.

The United States should take an expansive definition of what constitutes military necessity in regards to conducting offensive cyberoperations with the caveat that protected status for objects should be honored to the greatest extent possible. Merely interrupting or turning off certain functions for limited periods of time can ameliorate proportionality concerns. Planners should take caution when designing and conducting offensive cyberoperations so that ruses don't cross the line into perfidy. Reasonable efforts should be made to distinguish between military and civilian assets and between military personnel and civilians. Parallels can be used and interpreted regarding neutrality that will allow offensive cyberoperations to be used. Offensive cyberoperations can be used, in conjunction with the other theories of constraint, since no treaty exists that bans its use.

While an international treaty that spells out the limitations of offensive cyberoperations could prove somewhat helpful, it is highly unlikely that such an agreement will be reached. In the absence of an overarching agreement, the United States must look to existing frameworks and laws upon which to base its actions and ground them in international legitimacy. Using existing frameworks and laws and drawing analogous, reasonable interpretations of them will allow the United States to pursue its national security objectives.

Conclusion

The LOAC provides an analytical framework for planners and legal advisors to utilize when considering implementing various aspects of the military instrument of power to pursue national objectives. The use of a recognized analytical framework lends legitimacy to actions undertaken by the United States, and shows commitment to recognized rules of international law. Given the present parameters of the existing LOAC framework, parallel analogies and reasonable interpretations and applications of those analogies, the United States should legitimately be able to conduct the four types of offensive cyberoperations.

Notes

Bibliography

Andrew R. Kramer and Nicole Perlroth, *Expert Issues a Cyberwar Warning*, N.Y. Times (June 3, 2012) http://www.nytimes.com/2012/06/04/technology/cyberweapon-warning-from-kaspersky-a-computer-security-expert.html?pagewanted=all&_r=0

Anna Wortham, *Note: Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?* Federal Communications Law Journal vol. 64: 643 (May 2012)

Barton Gellman and Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show*, Washington Post, Aug. 30, 2013 (http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration)

Bradley Graham, "Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia," *Washington Post*, Nov. 8, 1999, A1.

Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post* (16 October 2008), found at http://voices.washingtonpost .com/securityfix/2008/10/report_russian_hacker_forums_ forums_f.html (accessed on 29 October 2013).

Bruno Waterfield, "EU blames Georgia for starting war with Russia," *The Telegraph*, 30 September 2009, http://www.telegraph.co.uk/news/worldnews/europe/georgia/6247620/EU-blames-Georgia-for-starting-war-with-Russia.html (accessed 29 October 2013).

C.J. Chivers, "Georgia Offers Fresh Evidence on War's Start," *New York Times*, 15 September 2008,

http://www.nytimes.com/2008/09/16/world/europe/16georgia.html?_r=2&oref=slogin& (accessed 29 October 2013)

CBS/AP, "China Stonewalls Panetta on Cyber Attacks." *CBS News*, 20 September 2012, http://www.cbsnews.com/8301-202_162-57516541/china-stonewalls-panetta-on-cyberattacks/ (accessed November 29, 2013)

Charles J. Dunlap, Jr., *Perspectives for Cyber Strategists on Law for Cyberwar*, Strategic Studies Quarterly 5, no. 1 (Spring 2011)

Curtis A. Bradley and Jack L. Goldsmith, *Customary International Law as Federal Common Law: A Critique of the Modern Position*, Harvard Law Review vol. 110, no. 4: 815 (February 1997)

David Goldman, *Major Banks Hit with Biggest Cyber Attacks in History*, *CNN.com*, September 28 2012, http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html (accessed November 29, 2013)

David Hollis, *Cyberwar Case Study: Georgia 2008*, Small Wars Journal Blog, January 6, 2011, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008, 1 (accessed October 6, 2013)

Duncan B. Hollis, *Why States Need an International Law of Information Operations*, Lewis and Clark Law Review, vol. 11: 1023 (2007)

Eric Talbot Jensen, *Cyber Deterrence*, Emory International Law Review vol. 26: 773 (2012)

Erick Mudrinich, *Article: Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, Air Force Law Review vol. 68:167 (2012)

Gabriel K. Park, *Note: Granting an Automatic Authorization for Military Response: Protecting National Critical Infrastructure from Cyberattack*, Brooklyn Journal of International Law, vol. 38: 797 (2013)

George K. Walker, *Information Warfare and Neutrality*, Vanderbilt Journal of Transnational Law vol. 33 no. 5: 1079 (November 2000)

Harold Hongju Koh, Remarks to the USCYBERCOM Inter-Agency Legal Conference, September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm (accessed November 29, 2013)

Heike Spieker, "Civilian Immunity," *Crimes of War: What the Public Should Know*. Roy Gutman and David Rieff, eds. (New York: W.W. Norton and Company, 1999), 84

Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, Journal of National Security Policy Law, vol. 4: 63 (2010)

House, *Statement of David Wheeler, Planning for the Future of Cyber Attack Attribution of the Subcommittee on Technology and Innovation on the Committee on Science and Technology*, 111th Cong.., 2nd sess., 2010, http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg57603/html/CHRG-111hhrg57603.htm (accessed November 29, 2013)

James Cook, *Cyberation and Just War Doctrine: A Response to Randall Dipert*, Journal of Military Ethics vol. 9, no. 4: 411 (2010)

Jan Arno Hessbruegge, *The Historical Development of the Doctrines of Attribution and Due Diligence in International Law*, New York University Journal of International Law and Politics, vol. 36: 265 (Winter/Spring 2004)

Jay P. Kesan and Carol M. Hayes. *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*. Harvard Journal of Law and Technology vol. 25, no. 2: 415 (Spring 2012)

Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, Inc., 2012)

Jeffrey T.G. Kelsey, *Note, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyberwarfare,* Michigan Law Review, vol. 106: 1427, 1437 (2008).

John Markoff and Andrew E. Kramer, "In Shift, U.S. Talks to Russia on Internet Security," *New York Times*, December 12, 2009, A1, http://www.nytimes.com/2009/12/13/science/13cyber.html?scp=l&sq=u.s.%20%20talks%20to%20russia%20on%20web%20security&st=cse.&_r=0) (accessed November 29, 2013)

John Markoff, "Before the Bombs, Cyberattacks." *New York Times*, August 13, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0 (accessed October 19, 2013)

John Richardson, *Article: Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, John Marshall Journal of Computer & Information Law vol. 29: 1 (Fall, 2011).

Jon Oltsik "Russian Cyber Attack on Georgia: Lessons Learned?" *Network World*, August 17, 2009, http://www.networkworld.com/community/node/44448 (accessed October 29, 2013)

Kristen Tullos, *Symposium: International Law and The Internet: Adapting Legal Frameworks in Response to Online Warfare and Revolutions Fueled by Social Media: From*

Cyber Attacks to Social Media Revolutions: Adapting Legal Frameworks to the Challenges and Opportunities of New Technology, Emory International Law Review vol. 26: 733 (2012)

Law of Armed Conflict Deskbook, International and Operational Law Department, (Charlottesville, VA: The United States Army Judge Advocate General's Legal Center and School, 2012), 138.

Lawrence T. Greenberg, Seymour E. Goodman and Kevin J. Soo Hoo, *Information Warfare and International Law* (Washington, DC: National Defense University Press, 1998), http://www.dodccrp.org/files/Greenberg_Law.pdf (accessed October 9, 2013)

Louis Henkin, ed. *Restatement of the Law Third, The Foreign Relations Law of the United States* (Philadelphia, PA: American Law Institute, 1989)

Louis René Beres, *Religious Extremism and International Legal Norms: Perfidy, Preemption, and Irrationality*, Case Western Reserve Journal of International Law, vol. 39: 709 (2007-2008).

Mark Rutherford, "Report: Russian mob aided cyberattacks on Georgia," *CNET News,* August 18, 2009, http://news.cnet.com/8301-13639_3-10312708-42.html (accessed on 29 October 2013)

Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Columbia Journal of Transnational Law, vol. 37: 885 (1998-1999)

Michael N. Schmitt. *Wired Warfare: Computer Network Attack and Jus in Bello*. International Review of the Red Cross vol.84, no. 846: 365 (2002)

Michael Walzer, "Responsibility and Proportionality in State and Nonstate Wars," Parameters vol. 39: 40-52 (Spring 2009).

Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, Journal of Conflict and Security Law, vol. 17, no. 2: 229 (Summer 2012) http://jcsl.oxfordjournals.org/content/17/2/229.full.pdf+html.

Nobuo Hayashi, *Requirements of Military Necessity in International Humanitarian Law and International Criminal Law*, Boston University International Law Journal vol. 28: 39 (2010)

Paul Ames, "EU: Most Russian cease-fire allegations overblown," *USA Today*, October 24, 2008, http://usatoday30.usatoday.com/news/world/2008-10-24-2937695828_x.htm (accessed 29 October 2013)

Randall R. Dipert, *The Ethics of Cyberwarfare*, Journal of Military Ethics vol. 9, no. 4: 384 (2010)

Richard DiMeglio, *The Evolution of the Just War Tradition: Defining Jus Post Bellum*, Military Law Review vol. 186: 116 (2005)

Robert D. Sloane, *Article, The Cost of Conflation: Preserving the Dualism of Jus ad Bello and Jus in Bello in the Contemporary Law of War*, The Yale Journal of International Law, vol. 34: 47 (2009)

Steven G. Bradbury, *Keynote Address: The Developing Legal Framework for Defensive and Offensive Cyber Operations*, Harvard National Security Journal, vol. 2: 591 (2011)

Susan W. Brenner, *'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare*, The Journal of Criminal Law & Criminology, vol. 97: 379 (2007)

Tod Leaven and Christopher Dodge, *The United States Cyber Command: International Restrictions vs. Manifest Destiny*, North Carolina Journal of Law & Technology, vol. 12: 1 (2010).

U.S. Department of Defense. Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (as amended through 15 August 2012)

Walter B. Huffman, *Margin of Error: Potential Pitfalls of the Ruling in The Prosecutor v. Ante Gotovina*, Military Law Review, vol. 211: 1 (Spring 2012)

William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, DC: National Academics Press, 2009)